AMENDMENTS TO CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A system for restoring a terminal having a display to a default condition when a clear file is downloaded to the terminal, comprising:

a random number generator included in the terminal; and

a file authentication arrangement for authenticating a clear file that is downloaded to the terminal from outside the terminal,

wherein said terminal is arranged to execute a clear instruction in said clear file upon authentication of said clear file,

wherein said clear file includes a random number generated by said random number generator ~~upon downloading of the clear file into the terminal~~ and displayed on said display so that the random number can be placed into the clear file before being downloaded to the terminal, and

wherein said random number is changed each time said terminal is restored to a default condition so as to prevent replay attacks resulting from copying of the clear file.

2. (Currently Amended) A system as claimed in claim 1, wherein said file authentication arrangement includes a private key for digitally signing said clear file, and a corresponding public key clear certificate containing information necessary to authenticate the digitally signed clear file.

3. (Canceled)

4. (Original) A system as claimed in claim ~~3~~ 2, wherein said clear certificate is a sponsor public key certificate stored in the terminal and corresponding to a signer certificate downloaded with the digitally signed clear file, said signer certificate corresponding to ~~a~~ said private key used to digitally sign said clear file.

5. (Original) A system as claimed in claim 2, wherein said private key is stored on a smartcard and is only accessible by a secure processor embedded in the smartcard.

6. (Original) A system as claimed in claim 5, wherein said sponsor public key certificate is stored in a read only memory in said terminal.

7. (Currently Amended) A system as claimed in claim 2, further comprising a file signing tool for digitally signing said clear file, said file signing ~~too~~ tool including a smartcard reader, and wherein all digital signing operations requiring access to said private key are carried out by a secure processor embedded in a smartcard inserted into said smartcard reader.

8. (Currently Amended) A system as claimed in claim ~~2~~ 7, wherein said smartcard further has stored thereon a signer certificate for authenticating said ~~digital signature~~ digitally signed clear file, and wherein said clear certificate authenticates said signer certificate.

9. (Original) A system as claimed in claim 8, wherein said signer certificate includes a file type field containing a clear string that controls clearing of the terminal in order to restore the terminal to its default status.

10. (Currently Amended) A method of restoring a terminal to a default condition, comprising the steps of:

generating a random number and storing the random number in a terminal;

displaying the random number on a display of the terminal;

placing the random number in a regular file following display of the random number;

digitally signing the regular file after placement of the random number to create a digitally signed clear file;

downloading the digitally signed clear file to the terminal;

authenticating the digitally signed clear file by comparing the digital signature with a corresponding value based on the stored random number;

restoring the terminal to a default condition;

generating a new random number and replacing the stored random number with the new random number after restoring the terminal to a default condition so as to prevent replay attacks resulting from copying of the digitally signed clear file.

11. (Original) A method as claimed in claim 10, wherein said step of placing the random number in a regular file comprises the steps of displaying the random number and inputting the random number to a filing signing tool.

12. (Original) A method as claimed in claim 10, wherein the step of digitally signing the regular file comprises the steps of inserting a smartcard having an embedded secure processor in a smartcard reader connected to the file signing tool, causing the secure processor to access the private key in order to generate the digital signature.

13. (Original) A method as claimed in claim 12, wherein the step of authenticating the digital signature comprises the step of authenticating the digital signature based on a signer public key certificate downloaded into the terminal together with the signed clear file.

14. (Original) A method as claimed in claim 13, wherein the step of authenticating the digital signature further comprises the step of retrieving a sponsor public key certificate from a read only memory in said terminal and authenticating the signer certificate using the sponsor public key certificate.

15. (Original) A method as claimed in claim 13, wherein the step of authenticating the digital signature based on the signer public key certificate comprises the steps of comparing a value derived from the digital signature using the signer public key certificate with a value derived from the stored random number to authenticate said clear file.

16. (Original) A method as claimed in claim 13, wherein the step of restoring said terminal to a default condition comprises the step of reading a clear string in a file type field of said signer public key certificate.

17. (Original) A method as claimed in claim 10, wherein said step of restoring said terminal to a default condition comprises the step of deleting a certificate tree from said terminal.